

### REMARKS

Reconsideration and allowance of this application are respectfully requested.

The Examiner indicated that claims 1-16 and 19 had been preliminarily amended. This is incorrect. The claim amendment filed with the Response to Restriction Requirement amended only claims 1 and 2. Claims 3-16 and 19 were not amended by that Response.

By this Amendment, claims 1 to 7 and 10-16 have been amended, claims 17-37 have been canceled, and new claims 38 to 47 have been added. No new matter has been added by these claims.

Claims 1-16 and 38 to 47 are pending in this application.

The Examiner objected to claims 1-16 for various informalities. In view of the above amendments, withdrawal of the claim objections is respectfully requested.

The Examiner rejected claims 8 and 9 under 35 U.S.C. §101 as hybrid claims. The Examiner also rejected claims 8 and 9 under §112, ¶2, and indicated that the §101 rejection would be withdrawn if the §112 rejection was overcome. The grounds for these rejections are respectfully traversed.

Claims 1, 8 and 9 are all method claims. Claims 8 and 9 depend from claim 1 and further limit the method of claim 1. Claim 1 recites a first trusted entity performing certain steps. Claim 8 further limits the method of claim 1 by requiring that the first trusted entity be “a module incorporating authentication, encryption or data signing capabilities in data communication with a computing device.” The recitation of structure in claim 8 does not make it a hybrid claim.

Similar arguments apply to claim 9.

Accordingly, withdrawal of these rejections under §§101 and 112 are respectfully requested.

### **THE PRIOR ART REJECTIONS**

The Examiner rejected claims 1-16 and 19 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,871,232 (Curie) in view of U.S. Patent Publication No. 2003/0093695 (Dutta). The grounds for this rejection are respectfully traversed in view of the above amendments and the following remarks.

Computer users in certain distributed computer networks (such as, e.g., peer-to-peer (P2P) networks) can benefit from sharing resources. For example, a particular computer in a P2P network may offer its storage to other computers in the network. Or a computer in a P2P network may let other computers use its processor or some other resources. The performance and functionality of many P2P networks improve as more computers in the networks share resources. The inventors realized that it would be desirable to reward computer users for sharing their computer resources with others. However, as the inventors also realized, neither the “buyer” nor the “seller” of a resource is a trusted party, and so any reward mechanism is subject to misuse and abuse. For example, if a first user claims to have allowed a second user to use his computer’s storage, some form of verification is needed to ensure that the first user is not paid (rewarded) if that claim is untrue (i.e., if the first user never made his storage available to the second user). (See generally discussion at ¶¶0009-0010.)

Thus, as stated in the Abstract of the Disclosure, “[t]he present invention is directed toward monitoring resource usage in an architecture where neither the resource buyer nor the resource seller can be trusted, and for rewarding benefits, compensation, or rewards based upon such monitored resource usage data. The system rewards users who offer to share the memory, storage, or bandwidth of

their computing resource to third parties within a distributed network.” “The present invention provides methods and systems for measuring resource usage in a distributed information network, where parties engaging in resource sharing transactions cannot be trusted, and for rewarding users who share resources.”

¶0018. (See also, ¶¶0039, 0047.)

In one aspect, the invention performs a redundancy check to ensure that a transaction is not a repeat transaction. This check prevents two computers from performing and being rewarded for multiple “sham” transactions.

The claims (as amended), clarify the roles of the various entities in the presently claimed invention. The claims, as amended, also clarify that the resource usage verification authority (RUVA) server uses the issued ticket and the modified ticket to determine the extent of resources provided by the second computer to the first computer. Since the modified ticket is modified by a trusted entity associated with the second computer, the RUVA server can rely on the information in the modified ticket to reflect what resources were actually provided by the second computer to the first computer. This approach prevents the second computer from obtaining unearned rewards.

Other aspects of the invention, e.g., as recited in claim 10, prevent the first and second computers from obtaining unearned rewards for simply repeatedly downloading a file. The redundancy check will detect such fraudulent attempts.

The Examiner acknowledges that Currie does not disclose modifying a ticket or comparing a ticket to a modified ticket. (*Office Action*, §12.) However, the Examiner asserts that Dutta overcomes the limitations in Currie. Applicant respectfully disagrees.

Dutta relates to secure handling of stored-value data objects, and, more particularly, to securely managing wireless device transactions involving stored

value data objects. *Dutta*, ¶0002. But Dutta lacks any teaching or suggestion of any system or method that measures the extent of resources provided by one computer to another in a distributed network.

The Examiner relies on Dutta ¶0045 supposedly to teach “utilizing said ticket and said modified ticket to determine the extent of resources provided by the second user to the first user.” What Dutta actually teaches in that cited portion is “rapid ticket verification,” which, as Dutta explains, “entails subjecting an electronic ticket to a high level of initial scrutiny ... and subsequently providing the user with a potentially less secure, short-lived, rapid verification object that may be verified more quickly than the original electronic ticket.” *Dutta* ¶0045. However, Dutta’s rapid ticket verification would not provide any information that would allow an RUVA server (or anything else) to “determine the extent of resources provided by the second computer to the first computer.” Dutta’s so-called “rapid verification object” is simply a ticket that can be quickly verified as a valid ticket. But validity of a ticket does not provide information about the extent of resources provided by one computer to another.

Since neither Dutta nor Currie teach or in any way suggest the claimed invention, withdrawal of this rejection under §103 is respectfully requested.

The Examiner rejected claims 10 and 11 under §103 as being unpatentable over Currie and Dutta and further in view of Terretta (U.S. Publication No. 2001/0047275).

Claims 10 and 11 depend from claim 1 and are therefore patentable over Currie and Dutta for at least the reasons given above. The Examiner applies Terretta to supposedly teach the claimed redundancy checks. As the Examiner notes, Terretta prevents a user from more than one simultaneous use of content. “If the user is already receiving / viewing content ..., the user is denied access to the newly requested content.” *Terretta* ¶0020. What Terratta tries to achieve is

“‘one ticket, one seat’.” *Terretta* ¶0022. Once a user disconnects from Terretta’s system, he can reconnect and download the same content. And in Terratta’s system, the same user can stay online and repeatedly download the same content.

Nothing in Terretta teaches or suggests, as recited in claim 11, “determining whether a file being accessed by the first computer has already been downloaded by said first computer.” Nor does anything in Terretta teach or in any way suggest “conducting a redundancy check.”

The purpose of these checks in the invention of claims 10 and 11 is not to prevent multiple downloads. Their purpose is to prevent a user from being rewarded for such downloads.

In view of the above, withdrawal of this rejection under §103 is respectfully requested.

In re PATENT Application of ROSE, Anthony

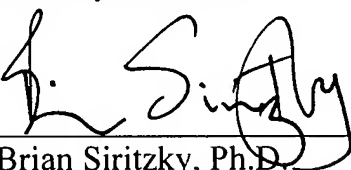
Appl. S.N.: 10/720,835

Page 13 of 13

### CONCLUSION

Applicant respectfully submits that this application is in condition for allowance, and an early action allowing the claims is earnestly solicited.

Should the Examiner believe that a telephone call will resolve any outstanding issues in this case, he is invited to telephone the undersigned at the number provided.

<b>CHARGE STATEMENT:</b> Deposit Account No. 501860, order no. 2618-0502.	
The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and which may be required under Rules 16-18 ( <u>missing or insufficiencies only</u> ) now or hereafter relative to this application and the resulting Official Document under Rule 20, or credit any overpayment, to our Accounting/Order Nos. shown above, for which purpose a <u>duplicate</u> copy of this sheet is attached	
<b>This CHARGE STATEMENT <u>does not authorize</u> charge of the <u>issue fee</u> until/unless an issue fee transmittal sheet is filed.</b>	
CUSTOMER NUMBER  <b>75948</b>	Respectfully submitted,  By:  _____ Brian Siritzky, Ph.D. Registration No.: 37,497
Davidson Berquist Jackson & Gowdey LLP 4300 Wilson Blvd., 7th Floor, Arlington, Virginia 22203 Main: (703) 894-6400 • FAX: (703) 894-6430	